(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 January 2003 (30.01.2003)

PCT

(10) International Publication Number
WO 03/009621 A1

(51) International Patent Classification[7]: H04Q 7/32, G06F 11/14, 1/16

(21) International Application Number: PCT/GB02/03287

(22) International Filing Date: 18 July 2002 (18.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

0117530.6	18 July 2001 (18.07.2001)	GB
0207932.5	5 April 2002 (05.04.2002)	GB
0207933.3	5 April 2002 (05.04.2002)	GB

(71) Applicants *(for all designated States except US)*: **MIATA LIMITED** [GB/GB]; 143 Charing Cross Road, London WC2H 0EH (GB). **WIZARD MOBILE SOLUTIONS LIMITED** [GB/GB]; 143 Charing Cross Road, London WC2H 0EH (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BLOCH, Stephen** [GB/GB]; 143 Charing Cross Road, London WC2H 0EH (GB). **DEMIRBASA, Saban** [GB/GB]; 143 Charing Cross Road, London WC2H 0EH (GB). **CURRY, Alistair** [GB/GB]; 143 Charing Cross Road, London WC2H 0EH (GB).

(74) Agents: **KAZI, Ilya** et al.; Mathys & Squire, 100 Grays Inn Road, London WC1X 8AL (GB).

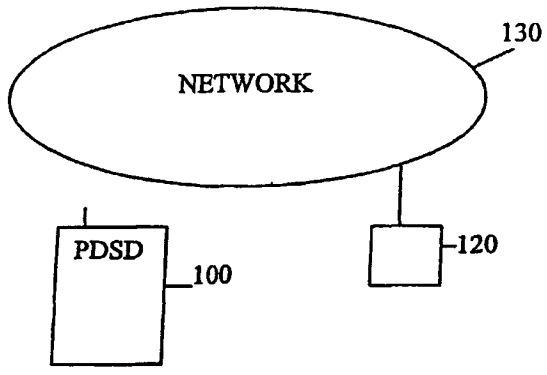
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PROTECTION OF DEVICES



(57) Abstract: A method of operating a portable data storage device or electrical equipment incorporating a communication module is disclosed. The method comprises initiating an alert procedure in response to a predetermined condition, the alert procedure comprising communicating a unique identifier of the portable data storage device or electrical equipment to a network. The identifier may then be used to locate and identify the portable data storage device or electrical equipment.

WO 03/009621 A1

Protection of Devices

The present invention relates to portable data storage devices and relates particularly to the detection or prevention of loss or theft of such devices.

In recent years, a significant decrease in the size of high technology devices which may be used to store and use data has allowed an increase in the portability of such devices and a proliferation in their use. Mobile telephone handsets, personal data assistants (PDAs) and handheld computers are just a few examples of data storage and utilisation devices that are commonly used and carried. As the use of such devices has grown, however, problems have arisen both in terms of loss of the data storage devices and their theft.

Individual manufacturers of the various portable devices have implemented mechanisms by which owners of a device may protect against the loss of information stored within the device and by which owners may protect against further use of the device once it has been stolen or lost. For example, many handheld computers are provided with a docking station via which data stored on the device may be downloaded and backed up to, for example a desktop computer. In the case of mobile telephones, a stolen or lost handset may be disabled by the mobile telecommunications network operator, since each mobile device has a unique International Mobile Equipment Identity (IMEI) number. If the IMEI number of a mobile handset is blocked from use on a mobile telecommunications network, then a stolen or lost handset may be rendered unusable.

The prior art solutions, however, require user input to ensure that data is backed up or that the device is rendered unusable after it has been lost or stolen. In addition, it may be possible for security features to be overcome, for example, the IMEI number of a mobile telephone may be altered by way of a relatively straightforward procedure, allowing a stolen mobile telephone to be used. Also, it may be possible to render a mobile telephone handset unusable, but the data stored on the handset may be lost if the handset is lost or stolen.

The present invention aims to provide a solution to the problems associated with the loss or theft of portable data storage devices, wherein the solution may be implemented over a wide range of storage devices.

According to a first aspect, there is provided a method of operating a portable data storage device, the method comprising initiating an alert procedure in response to a predetermined condition, the alert procedure comprising communicating a unique identifier of the portable data storage device to a network.

Communicating a unique identifier of the portable data storage device to a network may advantageously allow remote identification of the portable data storage device at which the alert procedure has been initiated. Identification of the portable data storage device at the network may occur immediately as the alert procedure is initiated, so there may be no delay in identifying the portable data storage device to the network once the alert procedure has been initiated. This may be faster and more reliable than, for example, waiting for the owner of the portable data storage device to identify the portable data storage device to the network.

Preferably, the method further comprises communicating periodically or quasi-continuously between the portable data storage device and a backup device over a wireless communication link.

More preferably, the predetermined condition comprises failure of the wireless communication link between the portable data storage device and the backup device for a predetermined period. Hence separation of the portable data storage device and the backup device for a predetermined period, for example due to theft or loss of the portable data storage device, may allow automatic initiation of the alert procedure. This may allow loss or theft of the portable data storage device to be noted as soon as the portable data storage device passes out of range of communication with the backup device. Again, this may remove the reliance on the owner of the portable data storage device to note the loss of the portable data storage device and to report that loss.

According to further embodiments, the predetermined condition may comprise conditions which arise in other situations, in addition to or in place of the condition outlined above. For example, the alert procedure may be initiated whenever an incorrect (or any) Personal Identification Number (PIN) is entered into the portable data storage device (for example, if a PIN is used to unlock the keypad of the portable data storage device). The alert procedure may be initiated periodically and automatically after a predetermined period. Switching on the portable data storage device may initiate the alert procedure, or the alert procedure may be initiated by a change in the location of the portable data storage device, for example, if the portable data storage device is a mobile telephone, this may comprise a change in the base station to which the mobile telephone is connected. The alert procedure may be initiated by a request from the network or upon the establishment of a call. The alert procedure may further be initiated when a portable data storage device, such as a mobile telephone, first connects to the network.

According to a highly preferable feature, the wireless communication link is a Bluetooth communication link. A Bluetooth link may provide a reliable link between the portable data storage device and the backup device and is suitable for use in communicating directly between the two devices over a short distance.

Preferably, the unique identifier of the portable data storage device is a Bluetooth serial number for the portable data storage device. As described in more detail below, each Bluetooth chip has a unique identifier, or serial number, which is difficult to alter. Hence the Bluetooth serial number may be used as a 'tag' for the portable data storage device.

The unique identifier may be communicated in addition to an International Mobile Equipment Identity (IMEI) number. Preferably, in at least one procedure in which the IMEI is communicated to a network, the unique identifier or a certificate based on the unique identifier (optionally in addition to an original IMEI number) is communicated in addition; this may enable the IMEI number to be authenticated.

According to a further preferable feature, the identifier of the portable data storage device comprises both a Bluetooth serial number and an International Mobile Equipment Identity (IMEI) number. This may allow the security of the system to be further increased since the identity of a portable data storage device may be verified more positively. In addition, the Bluetooth serial number may be verified against the corresponding IMEI number to ensure that the two numbers correspond to the same portable data storage device. This may allow the detection of portable data storage devices for which the IMEI number has been altered, which may allow the provision of the further feature that portable data storage devices that have not been identified to the network as being lost or stolen but which have been tampered with may be identified.

Preferably, a detection device may download the unique identifier of the portable data storage device from the network. This may allow the detection device to store a list of portable data storage devices that have been lost or stolen so that these portable data storage devices may be recovered if they are detected.

Preferably, the detection device queries the portable data storage device over a wireless communication link to obtain the unique identifier of the portable data storage device. The detection device may query any portable data storage device that is in range over a wireless communication link, such as a Bluetooth link. This may allow the detection device to identify any portable data storage device and may allow the user of the detection device to recover any portable data storage device listed as lost or stolen.

According to a further preferable feature, data stored in the portable data storage device is transferred to the backup device over the wireless communication link. Hence data stored in the portable data storage device may not be lost if the portable data storage device itself is lost or stolen. Transfer of data to the backup device may occur automatically at predetermined intervals, or may be initiated by the user of the portable data storage device. The data may include the unique identifier of the portable data storage device.

According to one preferable feature, the unique identifier of the portable data storage device is communicated to the network by the portable data storage device. Hence the portable data storage device may report its own loss or theft to the network on initiation of the alert procedure.

According to a further preferable feature, the unique identifier of the portable data storage device is communicated to the network by the backup device. This may occur in addition to, or instead of the portable data storage device reporting to the network. Hence this feature may act as a backup in case the portable data storage device itself cannot signal to the network. The network may be arranged to ignore a report received from a backup device if it has already received a report from the portable data storage device itself.

Preferably, the alert procedure further comprises communicating the unique identifier of the portable data storage device over a wireless communication link to a detection device. This may allow the identifier to be transmitted directly to any detection device that is within range of the portable data storage device or the backup device when the alert procedure is initiated. Hence any delay in detecting a lost or stolen portable data storage device may be minimised.

A second aspect provides a portable data storage device comprising:

means for storing a unique identifier;

means for implementing an alert procedure in response to a predetermined condition;

means for communicating the unique identifier to a network as part of the alert procedure.

The advantages of the second aspect and its preferred features are similar to the advantages of the corresponding features of the first aspect outlined above.

Preferably, the portable data storage device further comprises a Bluetooth chip, wherein the unique identifier is the Bluetooth serial number.

More preferably, the portable data storage device has an International Mobile Equipment Identity (IMEI) number, which is communicated to the network as part of the alert procedure in addition to the unique identifier.

Preferably, the portable data storage device further comprises means for communicating periodically or quasi-continuously with a backup device over a wireless communication link.

Further preferably, data stored within the portable data storage device is communicated to the backup device over a wireless communication link.

According to a further preferable feature the predetermined condition comprises failure of the wireless communication link between the portable data storage device and the backup device for a predetermined period.

Preferably, the wireless communication link between the portable data storage device and the backup device is a Bluetooth communication link.

A third aspect provides a method of detecting a lost or stolen portable data storage device comprising:

receiving at least one identifier of a portable data storage device over a wireless communication link;

determining whether the identifier of the portable data storage device corresponds to an identifier on a list of stolen or lost portable data storage devices.

As outlined above, this may allow lost or stolen portable data storage devices to be identified quickly and reliably. Since the method uses a wireless communication link, it is not necessary to establish physical connection to each portable data storage device.

Preferably, the method further comprises storing a list of identifiers of lost or stolen

portable data storage devices.

Preferably, the method further comprises requesting the at least one identifier of the portable data storage device over a wireless communication link. Using a wireless communication link, it is possible to 'scan' an area for portable data storage devices, requesting an identifier from each to identify any that are contained within the list.

Preferably, the wireless communication link is a Bluetooth communication link. As discussed above, a Bluetooth link may provide a reliable method by which short range communication may be established directly between Bluetooth devices.

Preferably, the at least one identifier of the portable data storage device is at least one of:

the Bluetooth serial number of the portable data storage device;

the IMEI number of the portable data storage device.

In the case of a mobile telephone, both identifiers may be provided for increased security.

Preferably, the list of identifiers of stolen or lost portable data storage devices is downloaded from a network. The network list may be updated automatically as portable data storage devices initiate an alert procedure, as described above. This list may then be periodically downloaded to detection devices, either over a physical link, or using a wireless communications link.

According to a fourth aspect, there is provided apparatus for detecting a lost or stolen portable data storage device comprising:

means for receiving at least one identifier of a portable data storage device over a wireless communication link;

memory means for storing a list of identifiers of stolen or lost portable data storage devices;

means for determining whether the received identifier of the portable data storage device corresponds to an identifier on the list of identifiers of stolen

or lost portable data storage devices.

Features of the third aspect outlined above may be applied to the fourth aspect. In the case of a Bluetooth or similar link, the apparatus may scan for lost or stolen devices in the vicinity and scanning devices may be given to enforcement agents and/or located in public places to trigger an alarm or to initiate an alert procedure on the device.

An audible alarm on the portable device may be triggered signifying to those in the vicinity that the device is stolen or lost; this may be triggered via a telecommunications network following receipt of the unique identifier or by a short range wireless communications link.

Preferably, the apparatus further comprises means for requesting the at least one identifier of the portable data storage device over a wireless communication link.

Preferably, the wireless communication link is a Bluetooth communication link.

According to a further preferable feature, the at least one identifier of the portable data storage device is at least one of:

the Bluetooth serial number of the portable data storage device;

the IMEI number of the portable data storage device.

Preferably, the apparatus further comprises means for downloading the list of identifiers of stolen or lost portable data storage devices from a network.

According to a fifth aspect, there is provided a method of verifying the identity of a portable data storage device comprising:

receiving, over a wireless communication link, an IMEI number for the portable data storage device;

receiving, over a wireless communication link, a further unique identifier for the portable data storage device;

verifying that the received IMEI number and the further unique identifier correspond to the same the portable data storage device.

Since the IMEI number of a portable data storage device may be altered according to a straightforward procedure, it is preferable if the identity of a portable data storage device can be verified using a combination of the IMEI number and another independent unique identifier. This may allow the identity of the portable data storage device to be ascertained more accurately and with more certainty and may allow the detection of devices that have been tampered with, or that have had their IMEI numbers altered. Receiving the required information over a wireless communication link may allow the detection to be performed remotely, so that a physical connection between the portable data storage device and the detection device is not required. This may allow verification of the identity of the portable data storage device without requiring the knowledge or co-operation of the user of the portable data storage device.

Preferably, the wireless communication link is a Bluetooth communication link. As discussed above, a Bluetooth link provides a reliable and easily implemented communications link over a short range between two devices.

Preferably, the further unique identifier is a Bluetooth serial number for a Bluetooth chip contained within the portable data storage device. As discussed above, each Bluetooth chip has a unique identifier, which it is difficult to alter. Hence the Bluetooth serial number may provide a suitable 'tag' for a Bluetooth-enabled portable data storage device.

Preferably wherein the step of verifying comprises checking the received IMEI number against the further unique identifier in a preexisting database. This database may be stored within the device that is verifying the identity of the portable data storage device, or may be accessed remotely by the verifying device.

Verification of the identity of the portable data storage device may be undertaken by

a network to which the portable data storage device is connected, or it may be undertaken by direct interrogation from a detection device, for example a handheld device carried by an authority such as the police.

Verification may take place automatically or periodically, or the process may be initiated in response to a predetermined condition or an alert procedure, such as one of the conditions or alert procedures outlined above for the first aspect. These predetermined conditions may include verifying the identity of a portable data storage device when it first connects to a network, or when it attempts to set up a connection (for example a mobile telephone call) across the network.

According to a further preferable feature, a certificate is generated for the portable data storage device if the received IMEI number and the further unique identifier correspond to the same portable data storage device. This may allow other devices to be sure that the identity of the portable data storage device has been correctly verified, and may mean that it is not necessary to verify the identity of the portable data storage device again at a later date. The verification device could simply check that the portable data storage device has been issued with a verification certificate.

A further aspect provides a method of operating a communication module, the method comprising initiating an alert procedure in response to a predetermined condition, the alert procedure comprising communicating a unique identifier of the communication module to a network.

Preferably, the communication module comprises means for operating a Bluetooth wireless communication link. However, the communication module may operate an alternative wireless communication link as outlined above for the portable data storage device.

Preferably, the method further comprises communicating periodically or quasi-continuously between the communication module and a base station device over a wireless communication link.

Preferably, the predetermined condition comprises failure of the wireless communication link between the communication module and the base station device. Alternative or additional predetermined conditions described for the first aspect may be applied to this aspect.

A further aspect provides apparatus comprising:
means for storing a unique identifier;
means for implementing an alert procedure in response to a predetermined condition;
a communication module for communicating the unique identifier to a network as part of the alert procedure.

Features of the previous aspect may be incorporated into the present aspect. In particular, the communication module may be a Bluetooth communication module and the unique identifier may be a Bluetooth serial number.

The apparatus may be advantageously manufactured to be very small and may be incorporated into a device such as a mobile telephone or a handheld computer. The apparatus may also be incorporated into electrical equipment, such as a video recorders or television set. The apparatus may be attached to or incorporated into clothing, or may be a discrete device in the form of a keyring, or an insert which would fit into a wallet. Hence the apparatus may be used to secure, for example, a bag, items of luggage, or a set of keys. The apparatus may also be incorporated into a larger item, such as a car or a bicycle. Preferably, the apparatus is incorporated into items that are likely to be lost or stolen, particularly high-value but portable items.

According to a further aspect, there is provided a method of compiling an inventory of at least one object, the or each object having an associated communication module the method comprising:
receiving, at a first communication module, a unique identifier of a communication module over a wireless communication link;

storing a list of the or each communication module unique identifier as an identifier of the corresponding object.

The or each communication module may comprise a Bluetooth communication module and the unique identifier for the or each communication module may comprise the Bluetooth serial number. The wireless communication link over which the or each unique identifier is received may also be a Bluetooth communication link.

The received identifiers may also be associated with further data about the devices which contain the communication modules correspond. This data may also be stored in the list or inventory alongside the received identifiers. For example, a description of the device containing each communication module may be stored in the inventory and data such as the time at which the unique identifier was first received or the time at which the unique identifier was last received may also be stored. Descriptions of the devices may be based on the identifiers received, hence it is the identifier that acts as the 'tag' for the device. The description of the devices corresponding to each identifier may be provided, for example, by the manufacturer. Since it is difficult to change a Bluetooth serial number, using this number as a 'tag' for the device may overcome problems associated with prior art inventory systems in which unauthorised amendments and alterations to the descriptions of devices and items may be made.

More than one unique identifier may be received from the or each further communication module, for example a mobile telephone may transmit its International Mobile Equipment Identity (IMEI) number.

Different types of unique identifier may be received from different communication modules (for example, a mobile telephone without a Bluetooth chip may transmit only its IMEI number) and unique identifiers may be received over different types of wireless communication links. For example, some unique identifiers may be received over a Bluetooth communication link, whereas other unique identifiers may be

received over a 802.11a or 802.11b wireless LAN link.

Unique identifiers of communication modules may be assembled automatically in a 'pull' method of operation. For example, the method may further comprise transmitting a signal to request identification numbers from any new communication modules that are within range. This may be done periodically, or on request from a user. Alternatively or in addition, a 'push' method of operation may be implemented, with communication modules automatically transmitting their unique identifiers. The method may further comprise providing the functionality to allow unique identifiers of communication modules to be added to the inventory manually, perhaps using an interface incorporated into, or attached to the first communication module (the first communication module being operable to implement the methods outlined above).

The method may also comprise the further functionality of the base station apparatus, which is outlined below.

A further aspect provides a base station which comprises:
a communication module for operating a wireless communication link to at least one further communication module;
memory means for storing an inventory of at least one unique identifier corresponding to the or each further communication module.

The base station may be suitable for implementing the method outlined in the previous aspect or any of its preferred features.

Preferably, the base station may further comprise means for monitoring the presence of the or each communication module corresponding to the or each unique identifier over a wireless communication link. The base station preferably periodically, or quasi-continuously, opens a wireless communication link to the or each communication module to ensure that the communication module is still within range of the base station. The identifier of any communication module that is not contactable over the wireless communication link may be added to a list of 'missing'

communication modules. This list may be stored within the base station or may be transmitted to a remote device or network, for example, the list may be accessible over the internet (preferably using a secure connection) or may be transmitted to a police database, or a database of an insurance company. A police database of identifiers of 'missing' communication modules may be used to identify stolen or lost communication modules, as described in more detail below. Identifiers of communication modules that are not contactable may be sent to a central database of 'missing' items. Descriptions of these items, based on the identifiers may also be stored in the database.

According to a further aspect, there is provided an inventory of at least one unique identifier, the or each unique identifier corresponding to a communication module, the inventory compiled by receiving, at a base station, the or each unique identifier over a wireless communication link.

Preferred features of the previous two aspects may also be applied to this aspect.

According to a further aspect, there is provided a detection device suitable for detecting at least one lost or stolen device containing a communication module, the detection device comprising:
means for receiving at least one identifier of the or each communication module over a wireless communication link.
means for determining whether the or each identifier corresponds to an identifier on a list of identifiers of lost or stolen communication modules.

The detection device may further comprise means for storing the list of identifiers of lost or stolen communication modules, or may comprise means for accessing the list if it is stored remotely. The detection device may further comprise means for requesting an identifier from a communication module over a wireless communication link. The communication module is preferably a Bluetooth communication module and the wireless communication link is preferably a Bluetooth communication link. The detection device may further comprise means

for obtaining the list of identifiers from a network, for example, via a computer connected to the internet.

A further aspect provides a method of detecting at least one lost or stolen device containing a communication module, the method comprising:
receiving at least one identifier of the or each communication module over a wireless communication link.
determining whether the or each identifier corresponds to an identifier on a list of identifiers of lost or stolen communication modules.

Preferred features of the detection device aspect outlined above may also be applied to this aspect.

A further aspect provides an electrical appliance with a communication module and a primary power supply, preferably an external power supply, wherein the communication module an internal power supply for supplying power to the communication module when the external power supply is not available, the internal power supply being sufficient to allow the communication module to transmit a unique identifier over a wireless communication link to a network in response to the initiation of an alert procedure.

The alert procedures outlined above may be applied to this aspect. The communication module is preferably a Bluetooth communication module and the unique identifier is preferably a Bluetooth serial number.

This aspect may allow communication from the appliance over the communication link even if the appliance does not have access to an external power supply. Hence communication may occur on the wireless communication link even if the appliance is left unplugged. This may be particularly useful in enabling an authority, such as the police, to identify stolen appliances that are not plugged in to a power supply.

The internal power supply preferably comprises a rechargeable power supply, such

as a rechargeable battery, which is preferably able to supply power to the communication module for a least a week when the external power supply is not available. More preferably, the rechargeable battery is able to supply power for a month. More preferably, the rechargeable battery is able to supply power for more than a month. More preferably, the rechargeable battery is able to supply power for more than six months. The battery may recharge automatically when the appliance is attached to the external supply.

The internal power supply may also allow other functions of the appliance to operate. Alternatively, the appliance may allow the internal power supply to be used only to transmit the unique identifier to a detection device. This may prevent the internal power supply being drained by being used to provide other functions of the appliance or communication module.

The internal power supply may further allow the appliance to enter a 'sleep' mode on disconnection from the primary power supply. The communication module in the appliance may wake from the sleep mode upon receipt of a request for its unique identifier, which may be received from a detection device.

In a further embodiment, the communication module may periodically transmit its identification number over the wireless communication link, in this way, the identifier of the communication module may be detected by any detection device within range.

A further aspect provides a method of operating a device containing a communication module comprising:

communicating a unique identifier of the communication module over a wireless communication link to a network;

receiving an activation signal to activate the device.

This may allow remote activation of a device, for example a device may be activated upon registration with the manufacturer, or may be activated at the point of sale.

The method may alternatively, or additionally comprise receiving a deactivation signal at the communication module over the wireless communication link to allow deactivation of the device. This may allow, for example, the police to deactivate stolen goods remotely, or may allow licensing authorities to deactivate goods for which a licence has not been paid, for example a television may be deactivated remotely if it does not have a corresponding television licence.

A description of one embodiment of the present application now follows. United Kingdom patent application GB 0117530.6, the contents of which are incorporated herein by reference, describes systems and methods by which data may be backed up periodically between a portable data storage device, such as a mobile telephone handset or a PDA, and a backup device over a wireless communication link. In addition, an alert procedure may be triggered in the backup device and/or in the portable data storage device if the portable data storage device goes out of range of the backup device. Example alert procedures may include the triggering of visible or audible alarms at one or both of the devices, rendering one or both of the devices unusable, for example by requiring the input of a code for their further uses, or alerting a network, for example a mobile telecommunications network. According to a preferable embodiment of the earlier application, the wireless communication link is a Bluetooth communication link.

An embodiment of the invention will now be described, by way of example, with reference to the accompanying drawings in which:

Fig. 1 shows a system in accordance with an embodiment of the present invention.

Fig. 2 shows an example of an alert procedure according to one embodiment of the present invention.

Fig. 3 shows a system in which the identity of a device may be verified.

The system shown in Fig. 1 comprises a portable data storage device 100, a backup device 110, a detection device 120 and a network 130 from which the detection device 120 may obtain information.

In this embodiment, the portable data storage device 100 is in the form of a mobile telephone and includes a short-range wireless communication interface, in this embodiment in the form of a Bluetooth transceiver chip. The transceiver may be integrated within the device itself, as in this embodiment, or may be provided as an additional component, which may then be integrated with the device or integrated with a battery for the device or within the battery housing. The device 100 stores contact details and optionally appointments or other data within the body of the device or on a SIM card provided with the device and a processor within the device 100 communicates with the communication interface.

Each Bluetooth chip has a unique Bluetooth serial number, which means that each device with an embedded Bluetooth chip has a unique Bluetooth identification number. If, as in this embodiment, the portable data storage device is a mobile telephone, the Bluetooth identification number is an identifying number additional to the IMEI number of the mobile telephone, discussed above. However, changing the Bluetooth serial number of a portable data storage device, for example a stolen mobile telephone handset, is a separate and a more difficult process than changing IMEI number. This may allow the Bluetooth serial number to be used as a tag for the portable data storage device.

The backup device 110 has a short-range wireless communication interface, in this embodiment in the form of a Bluetooth transceiver chip. An internal or external antenna may be provided, optionally on a circuit board. A processor may be used to control the operation of the backup device 110, specifically controlling communication via the interface. The short-range wireless communication interface of the backup device 110 may comprise means for receiving and storing the Bluetooth serial number of the portable data storage device 100.

The backup device may further comprise means to receive a user input 114 and an alarm device 112, for example a piezo electric sounder. A battery (not shown) may also be provided within the housing (although the device may, in some cases, be powered by the transmissions from the portable data storage device). The alarm

device may further include a visible alert or a vibrating alert device. The user input 114 means is preferably a simple input device, for example a single input button or a few buttons. A useful minimum function to implement with the user input device is cancelling of an alarm; other functions may be implemented by controlling the device via the communication interface. However, a more complex user interface may be provided, for example a voice recognition interface. In an alternative embodiment, the user interface may be omitted entirely; in such a case the alarm is preferably arranged to silence automatically after a predetermined time.

The backup device 110 optionally also includes backup data storage, for example FLASH memory. The amount of memory may be as little as 1Kb, for example to backup only key data but will typically be at least 64 Kbytes. Often considerably more memory, for example of the order of 1Mb to 10Mb and sometimes as much as 128Mb or even more may be provided, depending on the capacity of the device 100. The processor may further be used to control storage of data.

The backup device may be provided in a convenient housing, according to this embodiment the device is in the form of a key fob having a key ring 116 attached so that the device can conveniently be carried and is unlikely to be lost.

In an alternative embodiment, the device 110 may be attachable to or woven into an article of clothing, or may be incorporated into an alternative, preferably portable housing.

The detection device 120 preferably incorporates a short-range wireless communication interface, in this embodiment this is also a Bluetooth transceiver chip. In this embodiment, the detection device 120 further comprises means for communicating with a separate network 130. This may comprise means for communicating with the separate network 130 over a wireless communication link, but, in this embodiment, the detection device 120 comprises means to download data from the separate network 130 by connecting to a base station (not shown) in the separate network. The detection device 120 may connect to the base station

using a physical connection, or a wireless communication link, for example by using the short-range wireless communication interface. The detection device 120 further comprises means for storing data downloaded from the separate network, for example, the detection device may store a list of identifiers of lost or stolen portable data storage devices.

One example of an alert procedure which may be implemented by the embodiment shown in Fig. 1 will now be described with reference to Fig. 2.

In the example of Fig. 2, an alert procedure is triggered 200 by the portable data storage device passing out of the range of communication with the backup device. As described in more detail in United Kingdom patent application number GB 0117530.6, the alert procedure may be triggered when the portable data storage device moves a predetermined distance away from the backup device, or when the backup device is unable to maintain a communication link to the portable data storage device.

The alert procedure may involve the triggering of one or more of a visible, an audible or a vibrating alarm at the backup device 205, and/or at the portable data storage device, to alert the owner that the portable data storage device has passed out of range of the backup device. According to an additional, highly preferable feature, the portable data storage device may also be partially or fully disabled 210, for example by requiring a password or code before further use of the portable data storage device is possible.

According to this embodiment, the alert procedure comprises the further step of the portable data storage device sending a message to the separate network 215, the message containing an identifier of the portable data storage device, for example the Bluetooth serial number, or the IMEI number of the portable data storage device. The detection device may then receive the identifier of the lost of stolen portable data storage device 220. This may occur by the detection device downloading information from a base station connected to the mobile network.

The detection device may then send out query requests 225 to nearby portable data storage devices to which it may connect over a short-range wireless communication link, for example a Bluetooth link. These requests may allow the detection device to obtain the Bluetooth serial numbers of the nearby portable data storage devices, and optionally also the IMEI numbers of any nearby portable data storage devices that are also mobile entities. The Bluetooth serial numbers obtained may then be checked against the list of identifiers of stolen or lost portable data storage devices downloaded from the separate network. Hence, in this embodiment, the detection device may be used by an authority, such as the police, to detect and recover any lost or stolen portable data storage device.

According to a further feature of this embodiment, any IMEI numbers obtained for mobile entities may be checked against their corresponding Bluetooth serial numbers in a database, which may be stored within the detection device or accessed from a remote location by the detection device. Any portable data storage device for which the IMEI number does not correspond to the Bluetooth serial number may be cause further investigations to be initiated, since the IMEI number of the portable data storage device may have been altered. The true identity of the portable data storage device may be determined using the Bluetooth serial number, since this is more difficult to change than the IMEI number. If the IMEI number corresponds to the Bluetooth number, then a certificate may be generated and issued to the portable data storage device. This certificate may be used by other devices in connecting to the portable data storage device to ensure that the identity of ths portable data storage device has been successfully verified.

Verifying the identity of a portable data storage device, such as a mobile telephone, in the manner outlined above, may also be a process initiated by the network itself. The network may be prompted to verify the identity of the portable data storage device as part of an alert procedure such as one of the alert procedures outlined above, or, for example, when the portable data storage device registers with the network, or when the portable data storage device attempts to establish a call. If the network successfully identifies the portable data storage device and issues a

certificate, then the detection device may not need to repeat the procedure for that portable data storage device, but may simply check the certificate to establish the identity of the portable data storage device.

With reference to Fig. 3, the identity of a device, in this case a mobile telephone handset, may be verified in a number of different ways.

The handset 310 may transmit its SIM number 315, IMEI number 320, and Bluetooth serial number 325 to the network 300 individually for the network to verify the identity of the handset 310 and generate a certificate of identity. An alternative method, however, is for the handset 310 to generate an identity certificate itself from the SIM 315, IMEI 320 and Bluetooth 325 numbers and transmit this to the network 300. The network 300 may then verify the identity of the handset 310 without the handset having to transmit its actual SIM, IMEI and Bluetooth numbers. The certificate, or the individual numbers, may be encoded securely for transmission from the handset 310 to the network 300.

As an alternative to seizing a portable data storage device which has been lost or stolen, or which does not have an IMEI number corresponding to its Bluetooth serial number, the operator of the detection device, or the operator of the telecommunications network, in the case of a mobile telephone, may bar the portable data storage device from use.

According to a further embodiment, the system described above may operate in a symmetrical manner. For example, loss or theft of the backup device may also cause an alert procedure to be initiated, and the separate network may be informed of the Bluetooth serial number for the backup device, which may then be detected by the detection device and disabled or seized.

In addition, according to a further embodiment, the backup device may act as a backup device for a plurality of portable data storage devices, for example, a mobile telephone and a PDA of a user. Each portable data storage device may be

preregistered with the backup device, and the backup device may store the Bluetooth serial number for each portable data storage device. The backup device preferably allows wireless communications links to be set up from itself only to preregistered portable data storage devices. This may increase the security of any data stored within the backup device. An authorisation code or signal may be required to put the backup device into a registration mode in which new devices may register and pair with the backup device. Pairing attempts by unregistered portable data storage devices may be rejected, and an attempt by an unregistered device to pair with the backup device may cause an alert procedure to be initiated. This alert procedure may be the same as that outlined above, or may be a different alert procedure. For example, an unauthorised pairing attempt may simply cause a warning to be sent to the registered portable data storage device that the unauthorised attempt has been made.

The preceding description illustrates one embodiment of the present invention and modifications of detail may be provided.

Claims:

1. A method of operating a portable data storage device, the method comprising initiating an alert procedure in response to a predetermined condition, the alert procedure comprising communicating a unique identifier of the portable data storage device to a network.

2. A method according to Claim 1, further comprising communicating periodically or quasi-continuously between the portable data storage device and a backup device over a wireless communication link.

3. A method according to Claim 2 wherein the predetermined condition comprises failure of the wireless communication link between the portable data storage device and the backup device for a predetermined period.

4. A method according to Claim 2 wherein the wireless communication link is a Bluetooth communication link.

5. A method according to any preceding claim wherein the unique identifier of the portable data storage device is a Bluetooth serial number for the portable data storage device.

6. A method according to any preceding claim wherein the identifier of the portable data storage device comprises both a Bluetooth serial number and an International Mobile Equipment Identity (IMEI) number.

7. A method according to any preceding claim wherein a detection device may download the unique identifier of the portable data storage device from the network.

8. A method according to Claim 7 wherein the detection device queries the portable data storage device over a wireless communication link to obtain the

unique identifier of the portable data storage device.

9. A method according to any preceding claim wherein data stored in the portable data storage device is transferred to the backup device over the wireless communication link.

10. A method according to any preceding claim wherein the unique identifier of the portable data storage device is communicated to the network by the portable data storage device.

11. A method according to any of Claims 2 to 10 wherein the unique identifier of the portable data storage device is communicated to the network by the backup device.

12. A method according to any preceding claim wherein the alert procedure further comprises communicating the unique identifier of the portable data storage device over a wireless communication link to a detection device.

13. A portable data storage device comprising:
means for storing a unique identifier;
means for implementing an alert procedure in response to a predetermined condition;
means for communicating the unique identifier to a network as part of the alert procedure.

14. A portable data storage device according to Claim 13 further comprising a Bluetooth chip, wherein the unique identifier is the Bluetooth serial number.

15. A portable data storage device according to Claim 13 or 14 wherein the portable data storage device has an International Mobile Equipment Identity (IMEI) number, which is communicated to the network as part of the alert procedure in addition to the unique identifier.

16. A portable data storage device according to any of Claims 13 to 15 further comprising means for communicating periodically or quasi-continuously with a backup device over a wireless communication link.

17. A portable data storage device according to Claim 16 wherein data stored within the portable data storage device is communicated to the backup device over a wireless communication link.

18. A portable data storage device according to Claim 16 or 17 wherein the predetermined condition comprises failure of the wireless communication link between the portable data storage device and the backup device for a predetermined period.

19. A portable data storage device according to any of Claims 16 to 18 wherein the wireless communication link is a Bluetooth communication link.

20. A method of detecting a lost or stolen portable data storage device comprising:

receiving at least one identifier of a portable data storage device over a wireless communication link;

determining whether the identifier of the portable data storage device corresponds to an identifier on a list of stolen or lost portable data storage devices.

21. A method according to Claim 20 further comprising storing a list of identifiers which correspond to portable data storage devices which have been lost or stolen.

22. A method according to Claim 20 or 21 further comprising requesting the at least one identifier of the portable data storage device over a wireless communication link.

23. A method according to any of Claims 20 to 22 wherein the wireless communication link is a Bluetooth communication link.

24. A method according to any of Claims 20 to 23 wherein the at least one identifier of the portable data storage device is at least one of:
the Bluetooth serial number of the portable data storage device;
the IMEI number of the portable data storage device.

25. A method according to any of Claims 20 to 24 wherein the list of identifiers of stolen or lost portable data storage devices is downloaded from a network.

26. Apparatus for detecting a lost or stolen portable data storage device comprising:
means for receiving at least one identifier of a portable data storage device over a wireless communication link;
memory means for storing a list of identifiers of stolen or lost portable data storage devices;
means for determining whether the received identifier of the portable data storage device corresponds to an identifier on the list of identifiers of stolen or lost portable data storage devices.

27. Apparatus according to Claim 26 further comprising means for requesting the at least one identifier of the portable data storage device over a wireless communication link.

28. Apparatus according to Claim 26 or 27 wherein the wireless communication link is a Bluetooth communication link.

29. Apparatus according to any of Claims 26 to 28 wherein the at least one identifier of the portable data storage device is at least one of:
the Bluetooth serial number of the portable data storage device;

the IMEI number of the portable data storage device.

30. Apparatus according to any of Claims 26 to 29 further comprising means for downloading the list of identifiers of stolen or lost portable data storage devices from a network.

31. A method of verifying the identity of a portable data storage device comprising:
receiving, over a wireless communication link, an IMEI number for the portable data storage device;
receiving, over a wireless communication link, a further unique identifier for the portable data storage device;
verifying that the received IMEI number and the further unique identifier correspond to the same the portable data storage device.

32. A method according to Claim 31 wherein the wireless communication link is a Bluetooth communication link.

33. A method according to Claim 31 or 32 wherein the further unique identifier is a Bluetooth serial number for a Bluetooth chip contained within the portable data storage device.

34. A method according to any of Claims 31 to 33 wherein the step of verifying comprises checking the received IMEI number against the further unique identifier in a preexisting database.

35. A method according to any of Claims 31 to 34 wherein the method of verifying the identity of the portable data storage device is implemented by a network to which the portable data storage device is connected.

36. A method according to any of Claims 31 to 34 wherein the method of verifying the identity of the portable data storage device is implemented by

a detection device which interrogates the portable data storage device across a wireless communication link.

37. A method according to any of Claims 31 to 36 wherein a certificate is generated for the portable data storage device if the received IMEI number and the further unique identifier correspond to the same portable data storage device.

38. A method according to any of Claims 31 to 37 wherein the identity of the portable data storage device is verified in response to the initiation of an alert procedure.

39. A method of operating a communication module, the method comprising initiating an alert procedure in response to a predetermined condition, the alert procedure comprising communicating a unique identifier of the communication module to a network.

40. A method according to Claim 39 wherein the communication module comprises means for operating a Bluetooth wireless communication link.

41. A method according to Claim 39 or 40, further comprising communicating periodically or quasi-continuously between the communication module and a base station device over a wireless communication link.

42. A method according to any of Claims 39 to 41, wherein the predetermined condition comprises failure of the wireless communication link between the communication module and the base station device.

43. Apparatus comprising:
means for storing a unique identifier;
means for implementing an alert procedure in response to a predetermined condition;

a communication module for communicating the unique identifier to a network as part of the alert procedure.

44. A method of compiling an inventory of at least one object, the or each object having an associated communication module the method comprising:
receiving, at a first communication module, a unique identifier of a communication module over a wireless communication link;
storing a list of the or each communication module unique identifier as an identifier of the corresponding object.

45. A method according to Claim 44 wherein the or each communication module comprises a Bluetooth communication module.

46. A method according to Claim 45 wherein the unique identifier for the or each communication module comprises a Bluetooth serial number.

47. A base station, comprising:
a communication module for operating a wireless communication link to at least one further communication module;
memory means for storing an inventory of at least one unique identifier corresponding to the or each further communication module.

48. The base station according to Claim 47, further comprising means for monitoring the presence of the or each communication module corresponding to the or each unique identifier over a wireless communication link.

49. An inventory of at least one unique identifier, the or each unique identifier corresponding to a communication module, the inventory compiled by receiving, at a base station, the or each unique identifier over a wireless communication link.

50. A detection device suitable for detecting at least one lost or stolen device

containing a communication module, the detection device comprising:
means for receiving at least one identifier of the or each communication module over a wireless communication link;
means for determining whether the or each identifier corresponds to an identifier on a list of identifiers of lost or stolen communication modules.

51. A detection device according to Claim 50, further comprising means for requesting an identifier from a communication module over a wireless communication link.

52. A method of detecting at least one lost or stolen device containing a communication module, the method comprising:
receiving at least one identifier of the or each communication module over a wireless communication link;
determining whether the or each identifier corresponds to an identifier on a list of identifiers of lost or stolen communication modules.

53. An electrical appliance with a communication module and a primary power supply, preferably an external power supply, wherein the communication module has an internal power supply for supplying power to the communication module when the external power supply is not available, the internal power supply being sufficient to allow the communication module to transmit a unique identifier over a wireless communication link to a network in response to the initiation of an alert procedure.

54. An electrical appliance according to Claim 53, wherein the internal power supply comprises a rechargeable power supply.

55. An electrical appliance according to Claim 54, wherein the rechargeable power supply is able to supply power to the communication module for a least a week.

56. A electrical appliance according to Claim 54, wherein the rechargeable power supply is able to supply power to the communication module for at least a month.

57. A electrical appliance according to Claim 54, wherein the rechargeable power supply is able to supply power to the communication module for at least six months.

58. A electrical appliance according to any of Claims 54 to 57, wherein the rechargeable power supply recharges automatically when the appliance is attached to the external supply.

59. A method of operating a device containing a communication module comprising:
communicating a unique identifier of the communication module over a wireless communication link to a network;
receiving an activation signal to activate the device.

60. A method of operating a device containing a communication module comprising:
receiving a deactivation signal at the communication module over the wireless communication link;
deactivating the device in response to the deactivation signal.

61. A computer program or computer program product for implementing any of the methods herein described.

62. Apparatus substantially as herein described or as illustrated in any of the drawings.

63. Use of a Bluetooth serial number of an embedded communication module as a unique identifier to identify an object in which the communication module

is embedded.

Fig. 1

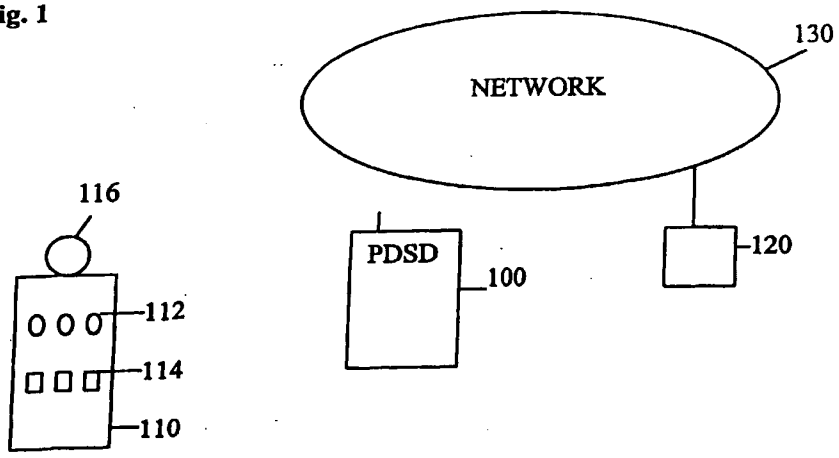

NETWORK
130
116
112
114
110
PDSD
100
120

Fig. 2

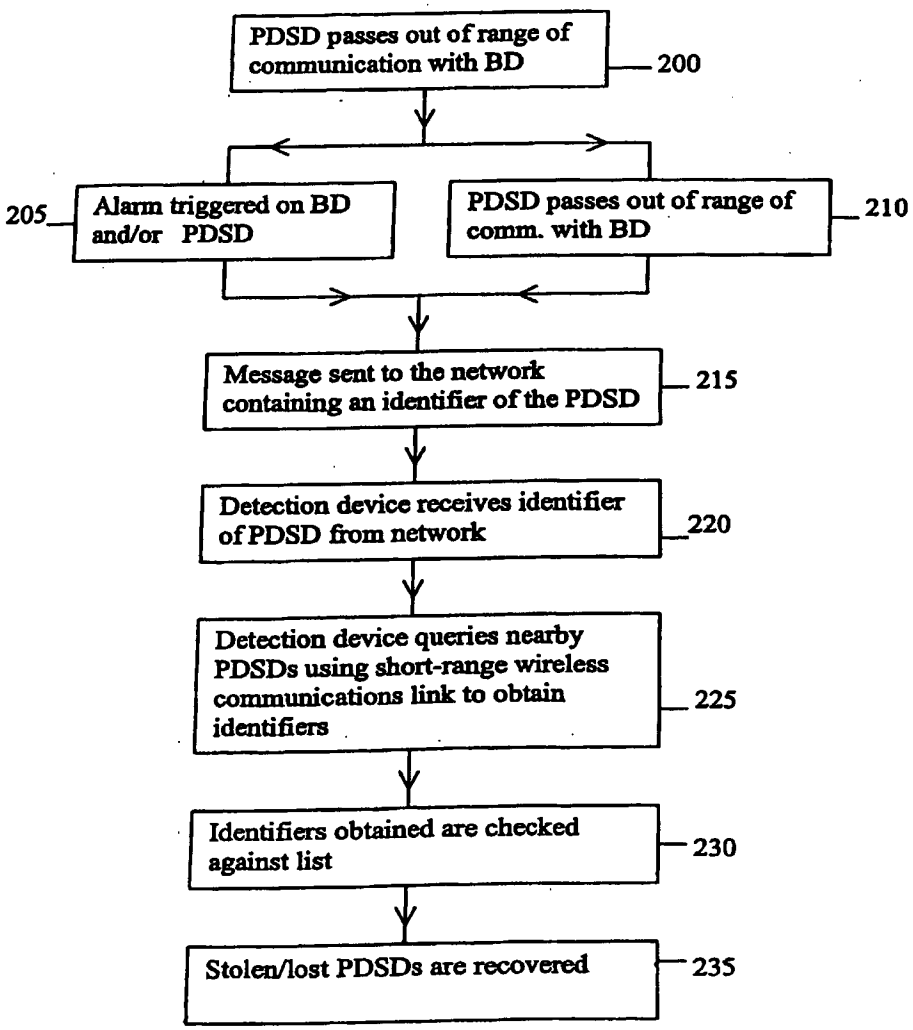
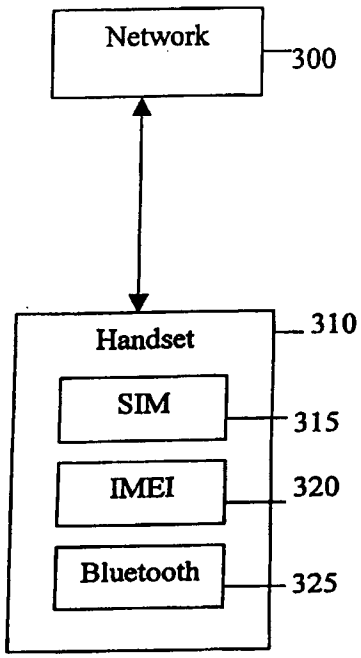

PDSD passes out of range of communication with BD
200
205
Alarm triggered on BD and/or PDSD
PDSD passes out of range of comm. with BD
210
Message sent to the network containing an identifier of the PDSD
215
Detection device receives identifier of PDSD from network
220
Detection device queries nearby PDSDs using short-range wireless communications link to obtain identifiers
225
Identifiers obtained are checked against list
230
Stolen/lost PDSDs are recovered
235

Fig. 3



INTERNATIONAL SEARCH REPORT

PCT/GB 02/03287

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/32 G06F11/14 G06F1/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 35304 A (NOKIA TELECOMMUNICATIONS OY ;AHVENAINEN JOUKO (FI)) 7 November 1996 (1996-11-07) page 3, line 16 -page 20, line 22 claims ---	1,10,12, 13,15, 20-22, 24,26, 27,29, 43,44, 47-52, 59-62
A	DE 199 56 851 A (SIEMENS AG) 31 May 2001 (2001-05-31) column 3, line 5 -column 4, line 51 claims --- -/--	1-63

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 December 2002	27/12/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Roberti, V

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 34631 A (ERICSSON TELEFON AB L M) 8 July 1999 (1999-07-08) page 4, line 21 -page 13, line 33	1-63
A	WO 00 45243 A (TELIA AB) 3 August 2000 (2000-08-03) page 10, line 15 -page 14, line 27	1-63
A	EP 1 102 191 A (NOKIA CORP) 23 May 2001 (2001-05-23) the whole document	1-63
A	EP 1 075 155 A (NOKIA MOBILE PHONES LTD) 7 February 2001 (2001-02-07) the whole document	1-63
A	GB 2 296 630 A (NIPPON ELECTRIC CO) 3 July 1996 (1996-07-03) the whole document	1-63

INTERNATIONAL SEARCH REPORT

PCT/GB 02/03287

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9635304	A	07-11-1996	FI	952146 A	05-11-1996
			AU	705416 B2	20-05-1999
			AU	5503596 A	21-11-1996
			CN	1183202 A	27-05-1998
			EP	0824838 A1	25-02-1998
			WO	9635304 A1	07-11-1996
			JP	11504481 T	20-04-1999
			NZ	306472 A	24-09-1998
			US	6148192 A	14-11-2000
DE 19956851	A	31-05-2001	DE	19956851 A1	31-05-2001
			WO	0138953 A1	31-05-2001
WO 9934631	A	08-07-1999	SE	517709 C2	09-07-2002
			AU	2082399 A	19-07-1999
			BR	9814560 A	16-10-2001
			CN	1290461 T	04-04-2001
			EE	200000344 A	15-08-2001
			EP	1025732 A1	09-08-2000
			JP	2002500492 T	08-01-2002
			SE	9704885 A	30-06-1999
			WO	9934631 A1	08-07-1999
			TR	200001774 T2	21-11-2000
			US	6334046 B1	25-12-2001
WO 0045243	A	03-08-2000	SE	515488 C2	13-08-2001
			WO	0045243 A1	03-08-2000
			SE	9900306 A	30-07-2000
EP 1102191	A	23-05-2001	EP	1102191 A2	23-05-2001
			JP	2001216187 A	10-08-2001
EP 1075155	A	07-02-2001	FI	991684 A	07-02-2001
			EP	1075155 A1	07-02-2001
GB 2296630	A	03-07-1996	JP	8181762 A	12-07-1996
			US	5875405 A	23-02-1999